What is claimed is:

1. A method of using a firewall to prevent spoofing of an address resolution cache of a host computer, the method comprising:

said firewall receiving an unsolicited message from a network that submits a new address resolution for a network protocol address;

said firewall checking independently cached address resolution information;

in response to determining that cached address resolution information for said network protocol address has an old address resolution which differs from said new address resolution, said firewall issuing a request for network elements having said network protocol address to reply with address resolution information;

in response to determining that no reply messages confirm that a network element has said old address resolution, said firewall permitting at least one message to pass onto said host computer which includes said new address resolution; and

in response to receiving a reply message that confirms a network element has said old address resolution, said firewall blocking at least one message which include said new address resolution from passing onto said host computer;

wherein said firewall protects said host computer from spoofed address resolution messages.

2. The method of claim 1, wherein said network implements a LAN network running Internet Protocol Version 4 using the Address Resolution Protocol (ARP) for resolving medium access control (MAC) addresses, and said address resolution cache is an ARP cache mapping IPv4 addresses to MAC addresses.

3. The method of claim 1, wherein said network implements Internet Protocol Version 6 (IPv6) with Neighbor Discovery for resolving MAC addresses, and said address resolution cache is a Neighbor Discovery cache for mapping IPv6 addresses to MAC addresses.

4. A method of using a firewall to prevent spoofing of an address resolution cache, the method comprising:

maintaining a shadow copy of said address resolution cache;

receiving an unsolicited message from a network that submits a new address resolution for a network protocol address;

checking said shadow copy of said address resolution cache;

in response to determining that cached address resolution information for said network protocol address has an old address resolution which differs from said new address resolution, issuing a request for network elements having said network protocol address to reply with address resolution information;

in response to determining that no reply messages confirm that a network element has said old address resolution, permitting an update of said address resolution cache to have said new address resolution; and

in response to receiving a reply message that confirms a network element has said old address resolution, blocking an update of said address resolution cache to have said new address resolution;

wherein the validity of an unsolicited address resolution is checked before permitting an update of said address resolution cache.

5. The method of claim 4, wherein said network implements a LAN network running Internet Protocol Version 4 using the Address Resolution Protocol (ARP) for resolving medium access control (MAC) addresses, and said address resolution cache is an ARP cache mapping IPv4 addresses to MAC addresses.

6. The method of claim 4, wherein said network implements Internet Protocol Version 6 (IPv6) with Neighbor Discovery for resolving MAC addresses, and said address resolution cache is a Neighbor Discovery cache for mapping IPv6 addresses to MAC addresses.

7. The method of claim 4, wherein said permitting said update of said address resolution cache comprises:

permitting a message having said new address resolution to pass onto a host computer.

8. The method of claim 4, wherein said blocking said update of said old address resolution comprises:

blocking at least one message having said new address resolution from passing onto a host computer.

9. The method of claim 4, wherein said maintaining said shadow copy comprises: storing cache entries with a residency lifetime greater than in said address resolution cache.

10. A firewall for preventing spoofing of an address resolution cache, comprising:

a state machine adapted to check independently cached address resolution information in response to receiving an unsolicited address resolution response message including a submitted address resolution for a network protocol address;

said state machine generating a request for network elements to report an address resolution for said network protocol address in response to determining that said address resolution of said unsolicited message differs from a previously cached address resolution for said network protocol address;

said state machine permitting an update of cached address resolution information to include said submitted address resolution in response to determining that no address resolution reply messages have said previously cached address resolution for said network protocol address; and

said state machine blocking an update of cached address resolution information to include said submitted address resolution for said network protocol address in response to determining a reply message has said previously cached address resolution.

11. The firewall of claim 10, further comprising: a shadow copy of said address resolution cache, wherein said state machine is adapted to check said shadow copy for cached address resolution information.

12. The firewall of claim 11, wherein cache entries in said shadow copy have a residency lifetime greater than corresponding entries of said address resolution cache.

13. The firewall of claim 10, wherein said address resolution cache is an ARP cache.

14. The firewall of claim 10, wherein said address resolution cache is a Neighbor Discovery cache.